

Computational tameness of classical non-causal models

Ämin Baumeler^{1,2} and Stefan Wolf^{1,2}

¹*Faculty of Informatics, Università della Svizzera italiana, Via G. Buffi 13, 6900 Lugano, Switzerland*

²*Facoltà indipendente di Gandria, Lunga scala, 6978 Gandria, Switzerland*

We show that the computational power of the non-causal circuit model, *i.e.*, the circuit model where the assumption of a *global causal order* is replaced by the assumption of *logical consistency*, is completely characterized by the complexity class $\text{UP} \cap \text{coUP}$. An example of a problem in that class is factorization. Our result implies that the non-causal model of classical closed timelike curves (CTCs) cannot solve problems that lie *outside* of that class. Thus, in stark contrast to other CTC models, these CTCs *cannot* solve NP-complete problems, unless $\text{NP} = \text{UP} \cap \text{coUP}$, which lets their existence in nature appear *less implausible*. This result gives a new characterization of $\text{UP} \cap \text{coUP}$ in terms of fixed points.

MOTIVATION AND RESULTS

The *acyclic* feature of “causality” [1], that an effect cannot be the cause of its cause, plays a central role in everyday live, physical theories, and models of computation. A *cyclic* causal structure is — in the classical meaning¹ of the following adjective — paradoxical. That may be a reason for why an *acyclic* notion is not only preferred but also a hidden assumption for many theories. Objections against *cyclic* causal structures are the *grandfather* and the *information antinomies* (see *e.g.* Refs [2, 3]). The former reads: By travelling to the past and killing his or her own grandfather, one could never have been born to travel to the past to kill his or her own grandfather. The latter is *ex nihilo* appearance of information, as illustrated in the following example. Assume one morning you wake up to find a proof of $\text{P} = \text{NP}$ on your desk. You decide to publish it and, after publication, you travel back in time to the night before you found the proof to place the original copy on your desk, while your younger self is asleep. Who wrote the proof?² However, if the proof you find on your desk is *uniquely* determined by a process, then the proof does not appear *ex nihilo*, but is the result of that process [5].

Closed timelike curves (CTCs) are loops in spacetime. That is, by traveling on such a curve, one would bump into oneself on the same position in space *and* time. Interestingly, CTCs appear as solutions to Einstein’s equations [6, 7], yet they have been or still are believed to be unphysical; their underlying structure is *cyclic*. For over twenty years people have studied different models of

CTCs and their implications. Echeverria, Klinkhammer, and Thorne [8] analyzed CTCs in the gravitational setting and showed that in *some* scenarios the grandfather antinomy is avoided. By Novikov’s principle [9], the scenarios where the grandfather antinomy arises are simply excluded. Deutsch [4] analyzed CTCs in the quantum information realm and showed that there, the grandfather antinomy *never* occurs. Because *multiple* consistent states to some initial conditions exist, Deutsch singles out the mixture of all consistent states that maximize the entropy as solution; by this he avoids the information antinomy. However, this maximum-entropy strategy has a price: The evolution becomes non-linear. Pegg [10] and others [11–15] designed a different model of CTCs, in which states are sent with the help of quantum teleportation to the past. That model, however, also leads to a non-linear evolution. Recently, Oreshkov, Costa, and Brukner [16] came up with a framework for quantum correlations without global causal order. There, the main assumptions are *linearity* and *local* validity of ordinary quantum theory. Interestingly, the framework describes correlations that cannot be simulated with a *global* causal order [16–19], and allows for advantages in query [20–24], as well as communication complexity [25, 26]. It was shown [19] that the classical spacial case [27] of that framework describes CTCs that avoid the grandfather *and* the information antinomies (we call such CTCs *logically consistent*). Furthermore, it can be used to define a *non-causal* circuit model of computation [28] that also avoids both antinomies.

Even though we do not know whether CTCs exist in nature or not, we can study their consequences. As Aaronson [29] put it, one could assume that nature *cannot* solve certain tasks (*e.g.*, NP-hard problems), in the same spirit as nature cannot signal faster than at the speed of light, and conclude that certain theories are *unphysical*. The same idea is used in reconstructions of quantum theory where the standard, unintuitive axioms are replaced by “more natural” ones (see *e.g.*, Refs. [30–49]). As it turns out [50], the class P_{CTC} of all problems solvable in polynomial time by classical Deutschian CTCs is equal to

¹ The noun “paradox” means a *seeming* contradiction as opposed to an *actual* contradiction. It originates from the Greek word *paradoxon* which is composed out of *para* (against) and *doxa* (opinion). We use the term *antinomy* for actual contradictions.

² Because it “contradict[s] the philosophy of science,” Deutsch [4] views this antinomy as by “far more serious” when compared to the grandfather antinomy. According to Deutsch, solutions to problems need to emerge through evolutionary or rational processes — otherwise the underlying theory would follow the *doctrine of creationism*.

its quantum analog BQP_{CTC} , and furthermore, equal to PSPACE .³ Most recently, Aaronson, Bavarian, and Gueltrini [52] showed that the Deutsch model can even solve the halting problem. The model of CTCs where the loops are generated through quantum teleportation to the past can solve all problems in the class $\text{PostBQP} = \text{PP}$ [13, 53, 54]. The classical analogue thereof can solve problems in BPP_{path} [13] — the classical analogue of PostBQP [55]. The inclusion relations between these classes are $\text{NP} \subseteq \text{PostBQP} \subseteq \text{P}_{\text{CTC}} \subseteq \text{EXP}$, where *strict* inclusions are conjectured. Our contribution is to show

$$\text{P}_{\text{NCCirc}} = \text{UP} \cap \text{coUP},$$

i.e., that the class P_{NCCirc} (NCCirc standing for “non-causal circuit”) of decision problems solvable in polynomial time with the non-causal circuit model is equal to $\text{UP} \cap \text{coUP}$. This class contains all decision problems where every answer (“yes” or “no”) has a *unique* witness. Examples of such problems are integer factorization [56] and parity games [57], casted as decision problems. Thus, the class $\text{UP} \cap \text{coUP}$ is of great importance to the field of cryptography. Our result implies that the logically consistent CTC model [19] cannot solve problems *outside* of $\text{UP} \cap \text{coUP}$. If we denote by P_{LCCTC} (LCCTC standing for “logically consistent CTC”) the class of decision problems solvable by the latter framework, then we have $\text{P} \subseteq \text{P}_{\text{LCCTC}} \subseteq \text{P}_{\text{NCCirc}} \subseteq \text{NP} \subseteq \text{PostBQP} \subseteq \text{P}_{\text{CTC}}$. This means that the logically consistent CTC model [19] is the weakest of all known CTC models in terms of computation, and is *unable* to solve NP -complete problems (unless $\text{NP} = \text{UP} \cap \text{coUP}$). We also show the analog statement for *search* problems: $\text{FP}_{\text{NCCirc}} = \text{F}(\text{UP} \cap \text{coUP}) = \text{TFUP}$, where TFUP is the class of all search problems with *unique* solutions. Furthermore, these results give an interpretation of the classes $\text{UP} \cap \text{coUP}$ and TFUP in terms of *fixed points*: Every instance of such a problem can be solved by finding a *unique* fixed point.

This work is organized as follows. First, we describe the computational model, and after that, we define some complexity classes and present our results. Then, we present an example on how to factorize integers by using that model, give conclusions, and state some open problems.

MODEL OF COMPUTATION

The non-causal circuit model, whose computational complexity we study, is based on the framework for cor-

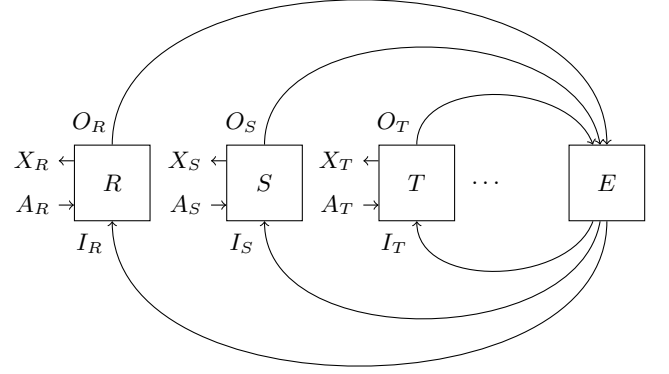


Figure 1. The parties R, S, T, \dots are modeled by stochastic operations $P_{X_V, O_V | A_V, I_V}$ for $V \in \{R, S, T, \dots\}$. The process matrix E (environment) is a channel (stochastic operation) $P_{I_R, I_S, I_T, \dots | O_R, O_S, O_T, \dots}$ that connects the outputs of the parties with their inputs.

relations without global causal order [16]. That framework is formulated in terms of *parties* and *process matrices*. In the *classical* special case [27] thereof, the parties and the process matrices model stochastic operations. A process matrix maps the *output* random variables of the parties to their respective *input* random variables (see Figure 1). A process matrix E is called *logically consistent* if and only if *any* choice of local operations of the parties R, S, T, \dots induces a probability distribution $P_{X_R, X_S, X_T, \dots, O_R, O_S, O_T, \dots | I_R, I_S, I_T, \dots | A_R, A_S, A_T, \dots}$. For deterministic process matrices (stochastic matrices with 0–1 entries only), the logical-consistency condition equals the requirement of a *unique fixed point* of the local operations composed with the process matrix, for *any* choice of local operations [58]. Formally, let

$$e : \mathcal{O}_R \times \mathcal{O}_S \times \mathcal{O}_T \times \dots \rightarrow \mathcal{I}_R \times \mathcal{I}_S \times \mathcal{I}_T \times \dots$$

be the function that represents the *deterministic* E , where \mathcal{O}_V and \mathcal{I}_V , for $V \in \{R, S, T, \dots\}$, are the sets of values the random variables O_V and I_V can take. Furthermore, we define the set \mathcal{F}_V as the set of *all* functions from \mathcal{I}_V to \mathcal{O}_V , *i.e.*, $\mathcal{F}_V = \{f_v : \mathcal{I}_V \rightarrow \mathcal{O}_V\}$. A *deterministic* E is called *logically consistent* if and only if

$$\forall r \in \mathcal{F}_R, s \in \mathcal{F}_S, t \in \mathcal{F}_T, \dots, \exists! (x_R, x_S, x_T, \dots) : (x_R, x_S, x_T, \dots) = e(r(x_R), s(x_S), t(x_T), \dots), \quad (1)$$

where $\exists!$ is the *uniqueness* quantifier. The condition of a unique fixed point ensures that the grandfather (*no* fixed point) and the information antinomies (*multiple* fixed points) are avoided.

The non-causal circuit model [28], then again, is formulated in terms of *gates* as opposed to *parties* and *process matrices*. A *circuit* is a collection of gates that are connected in an acyclic fashion, and where the input and

³ Some intuition behind this result is that Deutschian CTCs make time *reusable* just as space is, and thus a polynomial amount of space equals a polynomial amount of *reusable* time [51].

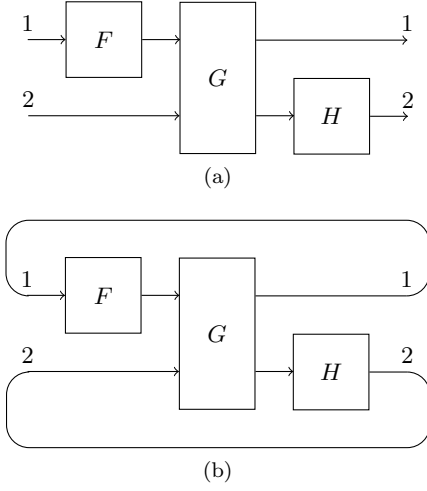


Figure 2. (a) Example of a circuit, where the input and output wires are labeled by 1, 2. (b) Closed circuit constructed from (a).

output wires are numbered from 1 on upwards in integer steps (see Figure 2a). Without loss of generality, and if not otherwise stated, we assume that every wire carries a bit. A *closed circuit* is a circuit without input and without output wires. A circuit \mathcal{C} with the same number of input and output wires is transformed to a closed circuit \mathcal{C}' by connecting all input and output wires with the same label (see Figure 2b). The introduced connections have to be thought as “back in time” if one presumes the existence of a global time. Let c be the function that is induced by the circuit \mathcal{C} . We call a closed circuit \mathcal{C}' *logically consistent* if and only if \mathcal{C} has a unique fixed point, *i.e.*,

$$\exists! x_0 : c(x_0) = x_0.$$

The difference between this model and the framework discussed above is that here, the circuit is *fixed* whereas in the framework, every party can *arbitrarily* choose its local operation. Thus we omit the all quantifier in the logical-consistency condition for circuits (compare the above Equation with Equation (1)). Logically consistent closed circuits can be used to find the unique fixed, which is exploited in the following.

COMPLEXITY CLASSES

A *decision problem* Π is often casted as the membership problem of a language $L \subseteq \Sigma^*$ with alphabet Σ . For simplicity, and without loss of generality, we choose $\Sigma = \{0, 1\}$. An instance of Π is a string $x \in \Sigma^*$, and the question is: Is x a word of L , *i.e.*, does $x \in L$ hold? An algorithm that solves a decision problem outputs either “yes” or “no.”

Search problems, then again, are mostly defined via binary relations. A problem Π is associated with a binary

relation $R \subseteq \Sigma^* \times \Sigma^*$. An instance of Π is some $x \in \Sigma^*$, and the question is: *What* (if there exists one) is $y \in \Sigma^*$ such that $(x, y) \in R$? An algorithm that solves a search problem outputs y if there exists a y satisfying $(x, y) \in R$, and returns “no” otherwise.

We use $|x|$ to denote the length of some string $x \in \Sigma^*$. A binary relation R is called *polynomially decidable* if there exists a deterministic Turing machine deciding the language $\{(x, y) \in R\}$ in polynomial time, and R is called *polynomially balanced* if $(x, y) \in R$ implies the existence of some polynomial q such that $|y| \leq q(|x|)$.

In the following definitions of complexity classes, we require that for every problem Π and given a string $x \in \Sigma^*$, we can check in polynomial time whether x is an instance of Π or not. If x is *not* an instance of Π , then we abort. We refer the reader to Refs. [59, 60] for common concepts in complexity theory.

Definition 1 (Deterministic NCCirc algorithm). A *deterministic NCCirc algorithm* \mathcal{A} is a polynomial time deterministic algorithm that takes as input some bit string $x \in \{0, 1\}^*$ and outputs a Boolean circuit \mathcal{C}_x over AND, OR, and NOT, such that for every x the closed circuit \mathcal{C}'_x is logically consistent, *i.e.*,

$$\forall x \in \{0, 1\}^*, \exists! y : c_x(y) = y.$$

If the fixed point y has the form $y = 1z$ for some z , then we say \mathcal{A} *accepts* x , otherwise, \mathcal{A} *rejects* x . The algorithm \mathcal{A} *decides a language* $L \subseteq \{0, 1\}^*$ if \mathcal{A} accepts every $x \in L$ and rejects every $x \notin L$. Furthermore, the algorithm \mathcal{A} *decides a binary relation* $R \subseteq \{0, 1\}^* \times \{0, 1\}^*$ if for every $x \in \{0, 1\}^*$ the pair (x, y) , with $c_x(y) = y$, is in R .

Based on the above definition, we define the complexity classes $\mathbf{P}_{\text{NCCirc}}$ and $\mathbf{FP}_{\text{NCCirc}}$.

Definition 2 ($\mathbf{P}_{\text{NCCirc}}$ and $\mathbf{FP}_{\text{NCCirc}}$). The class $\mathbf{P}_{\text{NCCirc}}$ contains all languages decidable by some deterministic NCCirc algorithm. The class $\mathbf{FP}_{\text{NCCirc}}$ contains all binary relations decidable by some deterministic NCCirc algorithm.

We will relate $\mathbf{P}_{\text{NCCirc}}$ to the following complexity class.

Definition 3 (UP). The class UP (Unambiguous Polynomial-time) contains all languages L for which a polynomial-time verifier $V : \{0, 1\}^* \rightarrow \{0, 1\}$ exists such that for every x , if $x \in L$ then $\exists! y : V(x, y) = 1$, and if $x \notin L$ then $\forall y : V(x, y) = 0$.

The complexity class UP was first defined by Valiant [61]. The only difference between the classes NP and UP is that in the former, *multiple* witnesses are allowed. The class coUP contains all languages L where the complement of L is in UP.

We are now ready to state our first theorem.

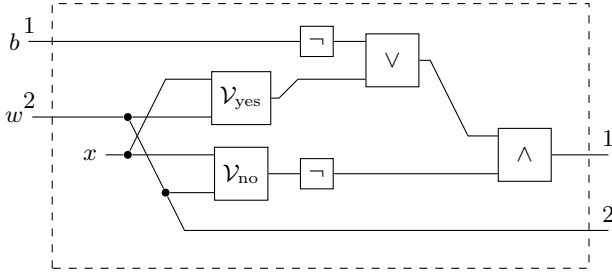


Figure 3. Circuit C_x used to reduce a problem from $\text{UP} \cap \text{coUP}$ to P_{NCCirc} . The wire that carries w consists of $q(|x|)$ bits.

Theorem 1. $\text{P}_{\text{NCCirc}} = \text{UP} \cap \text{coUP}$.

Proof. We start by showing $\text{UP} \cap \text{coUP} \subseteq \text{P}_{\text{NCCirc}}$. Assume a language L is in $\text{UP} \cap \text{coUP}$. Thus, there exist two polynomial-time verifiers V_{yes} and V_{no} such that for every x , if $x \in L$, then

$$\exists! w : V_{\text{yes}}(x, w) = 1 \wedge \forall w' : V_{\text{no}}(x, w') = 0,$$

and otherwise

$$\forall w : V_{\text{yes}}(x, w) = 0 \wedge \exists! w' : V_{\text{no}}(x, w') = 1.$$

The following deterministic NCCirc algorithm \mathcal{A} decides the language L . Upon receiving $x \in \{0, 1\}^*$, \mathcal{A} generates the circuit C_x as shown in Figure 3. The subcircuits $V_{\text{yes}}, V_{\text{no}}$ implement the verifiers $V_{\text{yes}}, V_{\text{no}}$, and can be constructed in polynomial time, because L is assumed to be in $\text{UP} \cap \text{coUP}$. The circuit acts in the following way:

$$c_x : \{0, 1\} \times \{0, 1\}^{q(|x|)} \rightarrow \{0, 1\} \times \{0, 1\}^{q(|x|)},$$

$$: (b, w) \mapsto \begin{cases} (0, w) & V_{\text{no}}(x, w) = 1, \\ (1, w) & V_{\text{yes}}(x, w) = 1, \\ (b \oplus 1, w) & \text{otherwise,} \end{cases}$$

where q is a polynomial. The function c_x has a *unique* fixed point. If $x \in L$, then there exists a unique w with $V_{\text{yes}}(x, w) = 1$, and $c_x(1w) = 1w$. Otherwise, there exists a unique w with $V_{\text{no}}(x, w) = 1$, and $c_x(0w) = 0w$.

The converse ($\text{P}_{\text{NCCirc}} \subseteq \text{UP} \cap \text{coUP}$) holds for the following reason. First, assume L is in P_{NCCirc} . This means that for every x we have some logically consistent circuit C'_x . We design both verifiers V_{yes} and V_{no} to act as

$$V_{\text{yes}} : (x, z) \mapsto c_x(z) = z \wedge z = 1w,$$

$$V_{\text{no}} : (x, z) \mapsto c_x(z) = z \wedge z = 0w.$$

That is, both verifiers just check whether z is a fixed point of C_x , and additionally check for the first bit. \square

Finally, we discuss the respective search problems.

Definition 4 (FUP). A binary relation R is in FUP (Function UP) if and only if R is polynomially decidable, polynomially balanced, and $\forall x : |\{y \mid (x, y) \in R\}| \leq 1$.

Informally, a problem is in FUP if for every instance there exists *at most* one solution.

Definition 5 ($\text{F}(\text{UP} \cap \text{coUP})$). A pair (R_1, R_2) of relations is in $\text{F}(\text{UP} \cap \text{coUP})$ if and only if both relations are polynomially decidable, polynomially balanced, and for every instance x

$$(\exists! y : (x, y) \in R_1 \wedge \forall z : (x, z) \notin R_2) \oplus$$

$$(\forall y : (x, y) \notin R_1 \wedge \exists! z : (x, z) \in R_2)$$

holds. The exclusive or (\oplus) asks for *either yet not both* expressions to be true.

Note that the output of a search problem in $\text{F}(\text{UP} \cap \text{coUP})$ is some string w that satisfies either $(x, w) \in R_1$ or (exclusively) $(x, w) \in R_2$ but, as we formulated it, does not tell us in *which* relation the pair (x, y) appears. However, since both relations are polynomially decidable, we can check in polynomial time whether y is a solution of R_1 or R_2 . This brings us to the following class, which is equal.

Definition 6 (TFUP). A binary relation R is in TFUP (Totally FUP) if and only if R is polynomially decidable, polynomially balanced, and $\forall x, \exists! y : (x, y) \in R$.

Theorem 2. $\text{TFUP} = \text{F}(\text{UP} \cap \text{coUP})$.

Proof. Let R be a relation in TFUP and R_1, R_2 two relations such that for every x :

$$(\exists! y : (x, y) \in R_1 \wedge \forall z : (x, z) \notin R_2) \oplus$$

$$(\forall y : (x, y) \notin R_1 \wedge \exists! z : (x, z) \in R_2).$$

To show $\text{TFUP} \subseteq \text{F}(\text{UP} \cap \text{coUP})$, set $R_1 = R$ and $R_2 = \emptyset$, and to show $\text{F}(\text{UP} \cap \text{coUP}) \subseteq \text{TFUP}$, set $R = R_1 \cup R_2$. \square

A similar statement $\text{TFNP} = \text{F}(\text{NP} \cap \text{coNP})$ can also be made [62]. The complexity class TFNP is the class of all *total* relations that are polynomially decidable and polynomially balanced.

We now state and prove the final theorem:

Theorem 3. $\text{FP}_{\text{NCCirc}} = \text{TFUP}$.

Proof. We start with $\text{TFUP} \subseteq \text{FP}_{\text{NCCirc}}$. A binary relation R in TFUP is polynomially decidable and polynomially balanced. Therefore, there exists an algorithm \mathcal{D} that takes two inputs x, y , runs in polynomial time in $|x|$, and if $(x, y) \in R$ then \mathcal{D} outputs “yes,” otherwise, \mathcal{D} outputs “no.” Furthermore, for every instance x there exists a *unique* y with $(x, y) \in R$. The deterministic NCCirc algorithm \mathcal{A} , upon receiving x , generates the circuit C_x that acts as

$$c_x : y \mapsto \begin{cases} y & (x, y) \in R, \\ y' & \text{otherwise,} \end{cases}$$

where, if $y = bz$ with $b \in \{0, 1\}$, then $y' = (b \oplus 1)z$. Thus, for every x we have a circuit \mathcal{C}_x with a unique fixed point that equals the solution, *i.e.*, $c_x(y) = y \rightarrow (x, y) \in R$. The converse inclusion relation $\text{FP}_{\text{NCCirc}} \subseteq \text{TFUP}$ is shown as follows. Suppose we are given a relation R that is decidable by a deterministic NCCirc algorithm \mathcal{A} . We now need to show that R is polynomially decidable, polynomially balanced, and that every x has a *unique* solution. Indeed, R is polynomially decidable and polynomially balanced because \mathcal{C}_x is generated in polynomial time, and \mathcal{C}_x upon input y is computed in polynomial time in $|x|$. Furthermore, \mathcal{C}_x has a *unique* fixed point. The algorithm \mathcal{D} to decide R on input x returns the truth value of $c_x(y) = y$. \square

EXAMPLE: INTEGER FACTORIZATION

We give an example of an algorithm to factorize integers. The NCCirc algorithm \mathcal{A} outputs, on input $N \in \mathbb{Z}$, a circuit \mathcal{C}_N with which $N = p_1^{e_1} p_2^{e_2} \dots$ can be decomposed into its prime factors p_1, p_2, \dots along with its exponents e_1, e_2, \dots . We give a description of \mathcal{C}_N as an algorithm. Clearly, this algorithm can be transformed into a circuit. The following algorithm runs in a time polynomial in $n = \lceil \log N \rceil$.

Algorithm 1 Factoring N

Input: $b \in \{0, 1\}, a_1, a_2, \dots, a_n, e_1, e_2, \dots, e_n \in K$
Output: $b' \in \{0, 1\}, a_1, a_2, \dots, a_n, e_1, e_2, \dots, e_n \in K$

```

1:  $w \leftarrow \neg b, a_1, a_2, \dots, a_n, e_1, e_2, \dots, e_n$ 
2: for  $i = 1$  to  $n - 1$  do
3:   if  $(a_i < a_{i+1}) \vee (a_i \neq 1 \wedge a_i = a_{i+1})$  then
4:     return  $w$ 
5:   end if
6: end for
7: for  $i = 1$  to  $n$  do
8:   if  $(a_i = 1 \wedge e_i > 1) \vee a_i \notin \text{PRIME} \cup \{1\}$  then
9:     return  $w$ 
10:  end if
11: end for
12: if  $a_1^{e_1} a_2^{e_2} \dots a_n^{e_n} \neq N$  then
13:   return  $w$ 
14: end if
15: return  $0, a_1, a_2, \dots, a_n, e_1, e_2, \dots, e_n$ 

```

Algorithm 1 takes as input 1 bit and $2n$ numbers in $K = \{1, 2, \dots, N - 1\}$, where every number is represented as an n -bit string. On line 3 we check whether the first n numbers are ordered. On line 8 we check whether e_i is 1 whenever $a_i = 1$, and whether a_i is indeed prime (or 1). A deterministic primality test can be performed in polynomial time as was recently shown [63]. Finally, on line 12 we check whether the decomposition is correct. If all tests are passed, then the algorithm returns $0, a_1, a_2, \dots, a_n, e_1, e_2, \dots, e_n$ where $\prod_{i=1}^n a_i^{e_i} = N$, otherwise, the algorithm *flips* the first input bit. This

algorithm and, therefore, the circuit \mathcal{C}_N , has a *unique* fixed point $0, p_1, p_2, \dots, p_m, 1^{n-m}, e_1, e_2, \dots, e_m, 1^{n-m}$, where $p_1 > p_2 > \dots > p_m$ are primes and $\prod_{i=1}^m p_i^{e_i} = N$. Intuitively, one can understand this algorithm as “killing the grandfather” whenever a wrong factorization is given.

CONCLUSION AND OPEN QUESTIONS

The non-causal circuit model describes circuits where the assumption of a *global causal order* is replaced by the assumption of *logical consistency* (*i.e.*, no grandfather and no information antinomies). The problems that are solvable in polynomial time by such circuits form the complexity class P_{NCCirc} . We show that this class equals $\text{UP} \cap \text{coUP}$, where UP consists of all problems in NP which have an *unambiguous* accepting path. Notable problems within $\text{UP} \cap \text{coUP}$ are integer factorization and parity games. Intuitively, the class P_{NCCirc} contains all search problems that can be solved by determining the *unique* fixed point of a specific reformulation of the problem. This gives a new interpretation of the class $\text{UP} \cap \text{coUP}$. The *uniqueness* requirement can be understood as arising from the assumption of no *overdetermination* (grandfather antinomy) and of no *underdetermination* (information antinomy). Similar complexity classes to $\text{FP}_{\text{NCCirc}}$ (the functional equivalent of P_{NCCirc}) are FIXP and linear-FIXP = PPAD [64]. These classes can solve problems where *multiple* fixed points might exist, and in FIXP, the fixed point are even allowed to be *irrational*. Finding a Nash equilibrium for two parties is linear-FIXP-complete, and the same problem for three parties or more is FIXP-complete [64]. The class $\text{P}_{\text{NCCirc}} = \text{UP} \cap \text{coUP}$ is not believed to contain *complete* problems [65].

This result leads us to conclude that closed timelike curves, based on the classical framework for correlations without global causal order, *cannot* solve problems outside of $\text{UP} \cap \text{coUP}$, *i.e.*, $\text{P}_{\text{LCCTC}} \subseteq \text{P}_{\text{NCCirc}}$. The reason for this is that in the CTC model we require the composed map of the parties with the environment to have a unique fixed point for *any choice* of local operations of the parties. This assumption was dropped when defining the non-causal circuit model. Thus, the CTC model is equal to the circuit model up to this additional condition, which can only lower the computational power. However, note the subtlety that the framework for classical correlations without causal order (as opposed to the CTC model) could, then again, solve problems not solvable by the CTC model. The reason for this is that in the correlations framework, *fine-tuned* process matrices are allowed [27] which are inherently probabilistic.

When we compare this result to the computational power of the Deutsch CTC model, we note that the CTC model studied here is *dramatically* weaker. This (possibly extreme) drop of computational power could be ex-

plained by the assumption of *linearity* which, in contrast to Deutsch’s model, is present in the model studied here. It is known that non-linearity can lead to astonishing results [66–68]. Put differently, the absence of the grandfather antinomy allows to solve problems in PSPACE, yet, if we additionally ask for the absence of the information antinomy, the complexity drops down to $UP \cap coUP$. As a side remark: The Deutsch version of CTCs restricted to *deterministic* fixed points gives a power of at most $NP \cap coNP$ [52].

One can put this result in the following perspective: Previous results on closed timelike curves show that they are not problematic from a general relativity theory point of view, from a logic point of view, and now we show their relative *innocence* from a computing of view.

Some of the main open questions that remain are: Does $P_{LCCTC} \supseteq P_{NCCirc}$ hold or not, what are the quantum versions BQP_{NCCirc} and BQP_{LCCTC} of the complexity classes defined here, and how does BQP relate to P_{NCCirc} ?

Acknowledgments. We thank Veronika Baumann, Gilles Brassard, Harry Buhrman, Paul Erker, Arne Hansen, and Alberto Montina for helpful discussions. We thank Claude Crépeau for his kind invitation to the 2016 Bellairs Workshop, McGill Research Centre, Barbados, where the main ideas emerged, and all participants of that workshop. This work was supported by the Swiss National Science Foundation (SNF) and the National Centre of Competence in Research “Quantum Science and Technology” (QSIT).

-
- [1] J. Pearl, *Causality: Models, reasoning, and interference*, 2nd ed. (Cambridge University Press, New York, 2009).
 - [2] S. Aaronson, “Why philosophers should care about computational complexity,” in *Computability: Turing, Gödel, Church, and beyond* (MIT Press, Cambridge, 2013) Chap. 10, pp. 261–327.
 - [3] J. Pienaar, *Causality Violation and Nonlinear Quantum Mechanics*, Ph.D. thesis, University of Queensland (2013).
 - [4] D. Deutsch, Physical Review D **44**, 3197 (1991).
 - [5] J.-M. A. Allen, Physical Review A **90**, 042107 (2014).
 - [6] K. Lanczos, Zeitschrift für Physik **21**, 73 (1924).
 - [7] K. Gödel, Reviews of Modern Physics **21**, 447 (1949).
 - [8] F. Echeverria, G. Klinkhammer, and K. S. Thorne, Physical Review D **44**, 1077 (1991).
 - [9] J. Friedman, M. S. Morris, I. D. Novikov, F. Echeverria, G. Klinkhammer, K. S. Thorne, and U. Yurtsever, Physical Review D **42**, 1915 (1990).
 - [10] D. T. Pegg, in *Time’s arrows, quantum measurement and superluminal behavior*, edited by D. Mugnai, A. Ranfagni, and L. S. Schulman (Consiglio Nazionale Delle Ricerche, Roma, 2001) p. 113.
 - [11] C. H. Bennett and B. Schumacher, “Simulated time travel, teleportation without communication, and how to conduct a romance with someone who has fallen into a black hole,” (2005), Talk at QUPON, 2005, Vienna, Austria.
 - [12] G. Svetlichny, preprint arXiv:0902.4898 [quant-ph] (2009).
 - [13] S. Lloyd, L. Maccone, R. Garcia-Patron, V. Giovannetti, and Y. Shikano, Physical Review D **84**, 025007 (2011).
 - [14] G. Svetlichny, International Journal of Theoretical Physics **50**, 3903 (2011).
 - [15] T. C. Ralph and T. G. Downes, Contemporary Physics **53**, 1 (2012).
 - [16] O. Oreshkov, F. Costa, and Č. Brukner, Nature Communications **3**, 1092 (2012).
 - [17] Ä. Baumeler and S. Wolf, in *2014 IEEE International Symposium on Information Theory* (IEEE, Piscataway, 2014) pp. 526–530.
 - [18] C. Branciard, M. Araújo, A. Feix, F. Costa, and Č. Brukner, New Journal of Physics **18**, 013008 (2015).
 - [19] Ä. Baumeler, F. Costa, T. C. Ralph, S. Wolf, and M. Zych, in preparation.
 - [20] G. Chiribella, Physical Review A **86**, 040301 (2012).
 - [21] T. Colnaghi, G. M. D’Ariano, S. Facchini, and P. Perinotti, Physics Letters A **376**, 2940 (2012).
 - [22] G. Chiribella, G. M. D’Ariano, P. Perinotti, and B. Valiron, Physical Review A **88**, 022318 (2013).
 - [23] M. Araújo, F. Costa, and Č. Brukner, Physical Review Letters **113**, 250402 (2014).
 - [24] L. M. Procopio, A. Moqanaki, M. Araújo, F. Costa, I. Alonso Calafell, E. G. Dowd, D. R. Hamel, L. A. Rozema, Č. Brukner, and P. Walther, Nature Communications **6**, 7913 (2015).
 - [25] A. Feix, M. Araújo, and Č. Brukner, Physical Review A **92**, 052326 (2015).
 - [26] P. A. Guérin, A. Feix, M. Araújo, and Č. Brukner, Physical Review Letters **117**, 100502 (2016).
 - [27] Ä. Baumeler and S. Wolf, New Journal of Physics **18**, 013036 (2016).
 - [28] Ä. Baumeler and S. Wolf, preprint arXiv:1601.06522 [quant-ph] (2016).
 - [29] S. Aaronson, Scientific American **298**, 62 (2008).
 - [30] C. Piron, Helvetica Physica Acta **37**, 439 (1964).
 - [31] C. Rovelli, International Journal of Theoretical Physics **35**, 1637 (1996).
 - [32] L. Hardy, preprint arXiv:0101012 [quant-ph] (2001).
 - [33] G. Brassard, H. Buhrman, N. Linden, A. A. Méthot, A. Tapp, and F. Unger, Physical Review Letters **96**, 250401 (2006).
 - [34] Č. Brukner and A. Zeilinger, Foundations of Physics **39**, 677 (2009).
 - [35] B. Dakić and Č. Brukner, in *Deep Beauty*, edited by H. Halvorson (Cambridge University Press, Cambridge, 2009) pp. 365–392.
 - [36] M. Pawłowski, T. Paterek, D. Kaszlikowski, V. Scarani, A. Winter, and M. Żukowski, Nature **461**, 1101 (2009).
 - [37] J. Rau, Foundations of Physics **41**, 380 (2011).
 - [38] G. Chiribella, G. M. D’Ariano, and P. Perinotti, Physical Review A **84**, 012311 (2011).
 - [39] B. Dakić, *Generic Probabilistic Theories — Reconstruction of quantum theory*, Ph.D. thesis, Universität Wien, Wien (2011).
 - [40] G. Chiribella, G. M. D’Ariano, and P. Perinotti, Entropy **14**, 1877 (2012).
 - [41] L. Masanes, M. P. Müller, R. Augusiak, and D. Perez-Garcia, Proceedings of the National Academy of Sciences

- 110**, 16373 (2013).
- [42] M. P. Müller and L. Masanes, *New Journal of Physics* **15**, 053040 (2013).
 - [43] N. Gisin, preprint arXiv:1407.8122 [quant-ph] (2014).
 - [44] D. Rohrlich, in *Quantum Theory: A Two-Time Success Story*, edited by D. C. Struppa and J. M. Tollaksen (Springer Milan, Milano, 2014) Chap. 13, pp. 205–211.
 - [45] G. Chiribella, G. M. D’Ariano, and P. Perinotti, in *Quantum Theory: Informational Foundations and Foils*, edited by G. Chiribella and R. W. Spekkens (Springer Netherlands, Netherlands, 2016) pp. 171–221.
 - [46] B. Dakić and Č. Brukner, in *Quantum Theory: Informational Foundations and Foils*, edited by G. Chiribella and R. W. Spekkens (Springer Netherlands, Netherlands, 2016) pp. 249–282.
 - [47] L. Hardy, in *Quantum Theory: Informational Foundations and Foils*, edited by G. Chiribella and R. W. Spekkens (Springer Netherlands, Netherlands, 2016) pp. 223–248.
 - [48] M. P. Müller and L. Masanes, in *Quantum Theory: Informational Foundations and Foils*, edited by G. Chiribella and R. W. Spekkens (Springer Netherlands, Netherlands, 2016) pp. 139–170.
 - [49] M. Pawłowski and V. Scarani, in *Quantum Theory: Informational Foundations and Foils*, edited by G. Chiribella and R. W. Spekkens (Springer Netherlands, Netherlands, 2016) pp. 423–438.
 - [50] S. Aaronson and J. Watrous, *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences* **465**, 631 (2009).
 - [51] S. Aaronson, “Time: Different from space,” <http://www.scottaaronson.com/blog/?p=368> (2008).
 - [52] S. Aaronson, M. Bavarian, and G. Gueltrini, preprint arXiv:1609.05507 [quant-ph], 29 (2016).
 - [53] S. Aaronson, *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences* **461**, 3473 (2005).
 - [54] S. Lloyd, L. Maccone, R. Garcia-Patron, V. Giovannetti, Y. Shikano, S. Pirandola, L. A. Rozema, A. Darabi, Y. Soudagar, L. K. Shalm, and A. M. Steinberg, *Physical Review Letters* **106**, 040403 (2011).
 - [55] Y. Han, L. A. Hemaspaandra, and T. Thierauf, *SIAM Journal on Computing* **26**, 59 (1997).
 - [56] M. R. Fellows and N. Kobitz, *Designs, Codes and Cryptography* **2**, 231 (1992).
 - [57] M. Jurdziński, *Information Processing Letters* **68**, 119 (1998).
 - [58] Å. Baumeler and S. Wolf, *New Journal of Physics* **18**, 035014 (2016).
 - [59] C. H. Papadimitriou, *Computational Complexity* (Addison-Wesley Publishing Company, San Diego, 1995).
 - [60] S. Arora and B. Barak, *Computational Complexity. A Modern Approach* (Cambridge University Press, New York, 2009).
 - [61] L. G. Valiant, *Information Processing Letters* **5**, 20 (1976).
 - [62] N. Megiddo and C. H. Papadimitriou, *Theoretical Computer Science* **81**, 317 (1991).
 - [63] M. Agrawal, N. Kayal, and N. Saxena, *Annals of Mathematics* **160**, 781 (2004).
 - [64] K. Etessami and M. Yannakakis, *SIAM Journal on Computing* **39**, 2531 (2010).
 - [65] M. Sipser, in *Automata, Languages and Programming* (Springer-Verlag, Berlin/Heidelberg, 1982) pp. 523–531.
 - [66] N. Gisin, *Physics Letters A* **143**, 1 (1990).
 - [67] J. Polchinski, *Physical Review Letters* **66**, 397 (1991).
 - [68] D. S. Abrams and S. Lloyd, *Physical Review Letters* **81**, 3992 (1998).